Commonwealth of Kentucky
Cabinet for Health and Family Services

Cabinet for Health and Family Services (CHFS) Information Technology (IT) Policy

040.301 Business Continuity Plan (BCP) Policy

Version 1.2
November 15, 2018

Revision History

Date	Version	Description	Author
9/16/2016	1.0	Effective Date	CHFS IT Policies Team Charter
11/15/2018	1.2	Review Date	CHFS OATS Policy Charter Team
11/15/2018	1.2	Revision Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
Executive Advisor (or designee)	11/15/2018	Jennifer Harp	Jennifer L. Harp
CHFS Chief Information Security Officer (or designee)	11/15/2018	DENNIS E. LEBER	D. E.

Table of Contents

1 Policy Definitions

- **Business Continuity Planning:** the creation of a strategy through the recognition of threats and risks facing a company, ensuring that personnel and assets are protected and able to function in the event of a disaster.
- **Business Continuity Plan (NIST):** The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes must sustain during and after a significant disruption.
- **Business Impact Assessment (BIA):** process that identifies and evaluates the potential effects (financial, life/safety, regulatory, legal/contractual, reputation and so forth) of natural and man-made events on business operations.
- **Confidential Data:** COT standards define confidential data as the data the Commonwealth has a legal obligation to not disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples include, but are not limited to, data not releasable under the Kentucky State law, Protected Health Information, Federal Tax Information, and Social Security and Credit Card Numbers.
- **Contract Staff/Personnel:** An employee hired through a state approved (i.e. System Design/Development Services {SDS} Vendor Agreement/Company) vendor who has a master agreement with the state.
- **Data Classification- NIST High Impact Level:** Severe or catastrophic effect on organizational operations, organizational assets, or individuals resulting in severe degradation to or a complete loss of an organization's ability to carry out its mission, severe financial loss, and/or catastrophic harm to individuals involving loss of life or serious life threatening injuries.
- **Data Classification- NIST Moderate Impact Level:** Serious adverse effect on organizational operations, organizational assets, or individuals including resulting in significant degradation to an organization's ability to carry out its mission, significant financial loss, and/or significant but non-life-threatening harm to individuals.
- **Data Classification- NIST Low Impact Level:** Limited adverse effect on organizational operations, organizational assets, or individuals resulting in minor degradation to an organization's ability to carry out its mission, minor financial loss, and/or minor harm to individuals.
- **Electronic Personal Health Information (ePHI):** Any protected health information (PHI) that is covered under Health Insurance Portability and Accountability Act of 1996 (HIPAA) security regulations and is produced, saved, transferred, or received in an electronic form.
- **Enterprise Identity Management (EIM):** Identity management solution used to provide internal users with network service entitlements.
- **Federal Tax Information (FTI):** Information received from the Internal Revenue Service (IRS) or secondary source, such as SSA, Federal Office of Child Support Enforcement or Bureau of Fiscal Service, that includes tax information. Examples would be an individual's tax return or anything that the IRS collects and that the IRS is going to use in order to determine a person's tax liability or potential tax liability.

- **Maximum Allowable Downtime (MAD):** The maximum period of time that a given business process can be inoperative before the organization's survival is at risk.
- **Personally Identifiable Information (PII):** Information used to distinguish or trace an individual's identity (i.e. name, Social Security number, biometric records, etc.). PII can be the individual's personal information or is identified when combined with other personal or identifiable information (i.e. date of birth, birthplace, mother's maiden name, etc.).
- **Recovery Point Objective (RPO):** The age of files that must be recovered from backup storage for normal operations to resume if a computer, system, or network goes down as a result of a hardware, program, or communications failure.
- **Recovery Time Objective (RTO):** The targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.
- **Sensitive Data:** Defined by COT standards, is data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include, but are not limited to, information identifiable to an individual (i.e. dates of birth, driver's license numbers, employee ID numbers, license plate numbers, and compensation information) and Commonwealth proprietary information (i.e. intellectual property, financial data, and more.)
- **State Staff/Personnel:** An employee hired directly through the state within the CHFS.
- **Vendor Staff/Personnel:** An employee contracted through an approved Master Business Associate Agreement, or other formal agreement, to provide temporary work for CHFS.

2 Policy Overview

2.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish comprehensive methodology for business continuity through a Business Continuity Plan (BCP). The BCP methodology must outline the crucial steps for agencies to recover and resume business functions in the event of a situation that disrupts, or threatens to disrupt agency business function(s). This document establishes the agency's BCP Policy and provides guidelines for security best practices regarding the establishment and implementation of a high-level BCP framework.

2.2 Scope

Each CHFS division is responsible for mapping out BCPs that are necessary to meet policy purpose listed above. The BCP must apply to all personnel, activities, and resources necessary to ensure recovery and normal resumption of business function/operations are achieved after disrupted or threatened with disruption. Designated personnel shall be familiar with the procedures and responsibilities within the BCP.

The scope of this policy applies to all internal CHFS state, contract, and vendor staff/personnel, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems.

2.3 Management Commitment

OATS Division Directors, the CHFS Chief Technical Officer (CTO), Chief Information Security Officer (CISO), and IT Executive Management have reviewed and approved this policy. Senior Management supports the objective put into place by this policy. Violations of not abiding by this policy may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. CHFS shall report illegal activities or theft of CHFS property (physical or intellectual) to the appropriate authorities.

2.4 Coordination among Organizational Entities

OATS coordinates with organizations and/or agencies with the cabinet, which access applications, systems, and facilities. All organizational entities that interact with CHFS are subject to follow requirements outlined within this policy.

2.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in applicable state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Applicable agencies additionally follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

3 Policy Roles and Responsibilities

3.1 Chief Information Security Officer (CISO)

Individual responsible for providing guidance and direction in assessment, planning, and implementation of all security standards, practices, and commitments required. This individual is responsible to adhere to this policy.

3.2 Chief Privacy Officer (CPO)

An individual responsible for overseeing activities related to the development, implementation, maintenance of, and adherence to the Cabinet's and Commonwealth's information privacy and confidentiality policies and procedures in compliance with federal and state laws. This individual will conduct Health Insurance Portability and Accountability Act (HIPAA) risk analysis through coordination with the Information Security Agency Representative, the CISO, or CHFS OATS Information Security (IS) Team, and other CHFS agencies, and will ensure compliance with HIPAA notification and reporting requirements in the event of an identified breach.

3.3 Security/Privacy Lead

Individual(s) designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate staff/personnel. This individual(s) is responsible for providing privacy and security guidance and direction for protection of Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff/personnel. This role along with the CHFS OATS IS Team is responsible for adherence to this policy.

3.4 CHFS Contract, State, and Vendor Staff/Personnel

All CHFS contract, state, and vendor staff/personnel must adhere to this policy. All staff/personnel must comply with referenced documents, found in section 8 Policy References below that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

3.5 System Data Owner and System Data Administrators

Management/lead who work with the application's development team to document components that are not included in the base server build and ensure functionality and backups are conducted in line with business needs. This individual(s) will be responsible to work with enterprise, agency, and application technical and business staff to provide full recovery of all the application functionality and meet federal and state regulations for disaster recovery situations.

3.6 Business Continuity Plan Coordinator

OATS Division of Strategic Services (DSS) individual(s) who help regularly coordinate all BCP activities by establishing, implementing, testing, training, maintaining the agency specific BCP, and ensuring audit compliancy along with the OATS IS Team.

3.7 Designated Agency Leads/Division Points of Contact

Individual(s) within, or outside of, the division that detects a situation or distribution and notifies appropriate parties. This position/role is a dedicated lead or group who is familiar with and adhere to the agency's BCP Procedures. The Designated Agency Lead(s) ensures the sustainment and delivery of business continuity and documentation for their agency, including testing, training, exercises, and updating (contact) information on an as needed basis.

3.8 Business Impact Analysis (BIA) Sponsor

Assist Coordinator to draft project work plan and draft BIA questionnaire. Complete BIA questionnaire. Assign other staff as necessary to complete project. Ach division will complete this process

4 Policy Requirements

4.1 Business Continuity Plan (BCP)

BCP methodology must align with standards within National institute of Standards and Technology (NIST) Special Publication 800-34 Revision 1, Contingency Planning Guide for Federal Information.

At a minimum, the following elements shall be documented and addressed within the plan:

1. Listing of Business Functions
2. Business Continuity Team Organization Chart
3. Roles and Responsibilities
4. Emergency Readiness Plan
5. Plan Phases (includes steps from initial notification through reconstitution)
6. Listing of Interoperable Communications
7. Plan for Safeguarding of Sensitive Documentation (FTI, Vitals, etc.)
8. Awareness, Training, Testing and Exercises

9. Emergency Contact Lists, both internal and external
10. Alternate Site(s) Information
11. Recovery Team Information
12. Report Forms

4.2 BCP Documentation Repository

Each agency is responsible for uploading, updating, and finalizing BCP documents and templates on a specified OATS SharePoint collection site. OATS will be responsible for the administering of the site, including the management of site membership. The agency's BCP Coordinator, Agency Leads, or designee, must keep a softcopy of the agency's BCP and templates at a designated off-site location for backup in case there is an incident or outage of the CHFS SharePoint site.

4.3 Business Impact Analysis (BIA) Mapping Requirements

BCP methodology must align with standards within National institute of Standards and Technology (NIST) Special Publication 800-34 Revision 1, Contingency Planning Guide for Federal Information. At a minimum, the following elements must be documented and addressed within the plan:

1. Develop the contingency planning policy;
2. Conduct the business impact analysis (BIA);
3. Identify preventive controls;
4. Create contingency strategies;
5. Develop an information system contingency plan;
6. Ensure plan testing, training, and exercises;
7. Ensure plan maintenance.

5 Policy Maintenance Responsibility

The OATS IS Team is responsible for the maintenance of this policy.

6 Policy Exceptions

Any exceptions to this policy must follow the guidance established in CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy.

7 Policy Review Cycle

This policy is reviewed at least once annually, and revised on an as needed basis.

8 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- Internal Revenue Services (IRS) Publication 1075
- Kentucky Revised Statute (KRS) Chapter 61.878 Certain public records exempted from inspection except on order of court – Restriction of state employees to inspect personnel files prohibited
- National institute of Standards and Technology (NIST) Special Publication 800-34 Revision 1, Contingency Planning Guide for Federal Information
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- Social Security Administration (SSA) Security Information